UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,778	02/14/2000	Paul Allen Cronce	429032000100	7144

29141 7590 02/10/2005

SAWYER LAW GROUP LLP
P O BOX 51418
PALO ALTO, CA 94303

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/503,778	CRONCE ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *19 July 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 28-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19 and 28-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☒ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. Claims 1-19, 28-45 are pending.

Response to Arguments

2. Applicant's arguments filed 7/19/04, have been fully considered but they are not persuasive.

Applicant has argued the following:

- *"Insofar as Caputo's device is for protecting access to a network through device/user identification and requires different methods/functionality to achieve that purpose, Caputo's device fails to solve the problem solved by the present invention, which is how to authorize the use of "software" and data on a computer in a manner that even an authorized user cannot make usable copies of the information being protected for an authorized user."*
- *"The device of the present invention and the device of Caputo have different purposes"*
- *"Caputo fails to teach or suggest the claimed invention, which authorizes the use of "software" and data on a computer, as claimed."*
- *"As stated above, Caputo's PINS fail to provide the same function as the claimed items of authorization information"*

- *"However, the purpose of Caputo's encryption is to simply encrypt information as it travels over the network. In contrast, the device of the present invention does not encrypt/decrypt information that is protected and authorized. Instead the protected information is stored on the computer awaiting authorization. Because the method and purpose of the device of the present invention are different from those of the Caputo device, this functionality is not needed in the present invention. In view of the foregoing, it is submitted claims 1-19 and 28-45 are allowable...."*

Applicant's arguments are general allegations that the function of Caputo is different from the functionality of the invention. Applicant appears to continue to argue that, because the functionality of purpose of Caputo, is different from the purpose of the present invention, Caputo is not applicable. Applicant has failed to provide any substantial evidence to support these allegations in the communication of 7/19/04. However, Applicant did make some clarifications in the telephonic interview of 2/4/05.

The Examiner contends Caputo meets the invention as set forth in the independent claims. Applicant has merely claimed "items of authorization information". The Examiner contends that Caputo's keys, PINS, and other secret information, is certainly information that is used for authorization purposes.

On 2/4/05, Applicant and Examiner engaged in a discussion concerning the nature of Applicant's invention as an improvement over a "dongle", portable devices specifically used to authorize

software. Applicant is thanked for this clarification and move to expedite prosecution. However, while the Examiner acknowledges that dongle elements, as discussed by the Applicant do appear to be present in the specification, these limitations, as discussed in the telephonic discussion, are not recited in the claims.

The Examiner therefore maintains the rejections as previously set forth.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-19, 28-29, 31-33, 35-45 are rejected under 35 USC § 102(b) as being anticipated by Caputo, US patent 5,778,071.

In reference to claim 1:

Caputo discloses a method for selectively authorizing a host system to use one or more items of protected information including software, where the software an application program (column 5, lines 7-12), comprising:

- Coupling the portable authorization device to the host system (Column 5, lines 57-64)
- Receiving a first item of authorization information from a first type of information authority, the first item of authorization information being associated with a first one of the items of protected information provided by a vendor of the first one of the items of

protected information, where the first item of authorization information is the Challenge, received from the Challenger, where the challenger is a vendor of this protected information. (Column 17, lines 33-56)

- Receiving a second item of authorization information from a second type of information authority, the second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected information, where the second item of authorization information is the PIN received from the user, where the PIN is provided by the user or a vendor of the Smartcards with PINs stored on them. (Column 17, lines 33-56) & (Column 14, lines 52-65)
- Selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information being stored therein, where the host system is authorized to use the one or more items of protected information, such as the application program, based upon the first or second item of authentication information, the PIN or the Challenge. (Column 17, lines 45-56)

In reference to claim 2:

Caputo discloses a portable authorization device for selectively authorizing a host system to use one or more items of protected information, including software, where the software is an application program (column 5, lines 7-12),

comprising:

- A processing unit; Caputo(Figure 2, Item 164)
- A storage medium operatively coupled to the processing unit; Caputo (Figure 2, Item 166)
- A first interface operative in conjunction with the processing unit and the storage medium for receiving a first item of authorization information from a first type of information authority, where the first interface is the smartcard interface and the first type of information authority is the smartcard. Caputo(Figure 2, Item 178)
    - The first item of authorization information being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information, where the first item of authorization information is the Challenge, received from the Challenger, where the challenger is a vendor of this protected information. (Column 17, lines 33-56)
- A second interface operative in conjunction with the processing unit and the storage medium for receiving a second item of authorization information from a second type of information authority, where the second interface is the Modem or network interface. Caputo(Figure 2, Item 160)
    - The second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected information, where the second item of authorization information is the PIN received from the user, where the PIN is provided by the user or a vendor of the Smartcards with PINs stored on them. (Column 17, lines 33-56) & (Column 14, lines 52-65)

- A third interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information being stored therein. Caputo(Figure 2, Item 12)
- Wherein the portable authorization device is removably couplable to the host system through the third interface. Caputo(Figure 2, Item 12) & Caputo(Figure 1A, Item 12)

In reference to claim 3:

Caputo discloses a device wherein:

- The first interface comprises a direct information authority interface program. Caputo(Column 10, lines 24-21)
- The first type of information authority comprises a direct information authority operatively coupled directly to the portable authorization device Caputo(Figure 1C)
- The second and third interfaces each comprise a same host system interface program. Caputo(column 9, lines 28-32)
- The second type of information authority comprises an indirect information authority operatively coupled directly to the portable authorization device, where the indirect information authority is a network that is operatively coupled to the device. Caputo(Figure 3)

In reference to claim 4:

Caputo discloses a portable authorization device, wherein the indirect information authority comprises a computer system coupled to the host system via a network. Caputo(Figure 3)

In reference to claim 5:

Caputo disclose a portable authorization device, wherein the indirect information authority comprises data stored on a magnetic storage medium, where the magnetic storage medium may be information stored on another computer on the network. Caputo(Figure 3, Item 36)

In reference to claim 6:

Caputo disclose a portable authorization device further comprising:

- A host authorizer operative in conjunction with the processing unit and the third interface for selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information,

where the network or computer is made accessible once the verification process is successful, and the authorizer acted in response to information from the smartcard and/or network and other information sources. Caputo(column 17, lines 51-56)

In reference to claim 7:

Caputo(column 9, lines 28-32) disclose a device wherein the host authorizer is a software program operatively stored in the storage unit.

In reference to claim 8:

Caputo discloses a device wherein:

- The first and second items of authorization information comprise first and second key selectors, respectively, where the first information authority, the smartcard, and the second information authority, the network, both contains a key selectors. Caputo (Column 14, lines 55-57) & (Column 17,lines 44-54)
- The host authorizer in conjunction with the processing unit and the third interface operatively generates a key based upon the first of second key selectors and selectively authorizes the host system to use the one or more items of protected information based upon the key, where the host authorizer responds to the challenge by establishing or "generating" the right key and then returned to the challenger that the device possesses the right key. If verification is successful, the network may authorize the host system to use the items of protected information, the accessibility of the network, or computer software. Caputo(Column 17, lines 37-56)

In reference to claim 9:

Caputo disclose a portable authorization device, wherein:

the first interface is configured to conduct a challenge response transaction with the first type of information authority, where the first information authority is the smartcard, and the first interface is the Item 178 of Figure 2, the smartcard interface. Caputo (Column 17, lines 37-44)

In reference to claim 10:

Caputo discloses a portable authorization device wherein:

the second interface is configured to conduct a challenge-response transaction with the second type of information authority, where the second interface is the network interface which receives the challenge from the network and the second type of information authority is the network. Caputo (Column 17, lines 30-35)

In reference to claim 11:

Caputo discloses a portable authorization device wherein:

the third interface is configured to conduct a challenge-response transaction with the host system, where the third interface is the interface that communicates with the host system and passes an acknowledgement to the host system as part of the challenge-response transaction. (Column 17, lines 51-56)

In reference to claim 12:

Caputo discloses an authorization system for selectively authorizing a host system to use one or more items of protected information, comprising:

- An access control mechanism associated with the host system for receiving a first item of authorization information from a first type of information authority operatively coupled to the host system and for forwarding the item of authorization information to the portable authorization device, where the host system receives items of authorization information from an information authority, or user, and the information is sent to the device. Caputo (Column 15, lines 19-24)

- The first item of authorization information being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information, where the first item of authorization information is the Challenge, received from the Challenger, where the challenger is a vendor of this protected information. (Column 17, lines 33-56)

- A portable authorization device removably couplable to the host system for receiving the first item of authorization information from the access control mechanism and for selectively authorizing the host system to use the one or more items of protected information based upon the first item of authorization information being stored therein, where the device receives the information from host system, and the end result of the device is to authorize the host system to use one or more items of protected information, such as the transmission of encrypted data Caputo (Column 15, lines 19-24), and where the data stored therein is the PIN and stored in the device. (Column 14, lines 52-65)

In reference to claim 13:

Caputo discloses an authorization system wherein:

- The portable authorization device is configured to also receive a second item of authorization information from a second type of information authority operatively coupled to the portable authorization device and, the second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected

information, where the second item of authorization information is the PIN received from the user, where the PIN is provided by the user or a vendor of the Smartcards with PINs stored on them. (Column 17, lines 33-56) & (Column 14, lines 52-65)

- And furthermore, is configured to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information, where the device, referred to as "device 10" in Caputo, may additionally accept authorization information from a smartcard. (Caputo Figure 1C)

In reference to claim 14:

Caputo discloses a portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

- A processing unit; Caputo(Figure 2, Item 164)
- A storage medium operatively coupled to the processing unit; Caputo (Figure 2, Item 166)
- A first interface operative in conjunction with the processing unit and the storage medium for receiving a key selector from an information authority; Caputo(Figure 2, Item 178) where the first interface is the smartcard interface, the storage medium and the information authority are the smartcard.
    - The key selector being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected

information, where the key selector is the PIN that unlocks the private key. (Column 14, lines 52-65)

- A host authorizer operative in conjunction with the processing unit and the storage medium for generating a key based upon the key selector. Caputo(Figure 8, Item 128)
- A second interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the key. Caputo (Figure 2, Item 174)

In reference to claim 15:

Caputo discloses a portable authorization device wherein:

- The first interface comprises an information authority interface; Caputo(Figure 2, Item 178)
- And the second interface comprises a host system interface. Caputo(Figure 2, Item 174)

In reference to claim 16:

Caputo discloses a portable authorization device for selectively authorizing a host system to use a plurality of items of protected information, comprising:

- A processing unit ; Caputo(Figure 2, Item 164)
- A storage medium operatively coupled to the processing unit for storing one or more items of blended authorization information, each item of blended authorization

information being derived from a plurality of items of authorization information, where the storage medium is the ROM/RAM and stores items of blended information that may be received from a network, a user, a smartcard, or the host computer. Caputo(Figure 2, Item 166)

- An unblending mechanism operative in conjunction with the processing unit and the storage medium for regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information, where the authorization information is processed and "unblended" into the conceptual diagram of figure 4B, where the authorization information is encrypted or decrypted and where the private key may be "regenerated" when needed in the authorization process. Caputo(Figure 4B)
- A host system interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information Caputo(Figure 2, Item 174)
- Wherein the portable authorization device is removably couplable to the host system through the host system interface. Caputo(Figure 1D, Item 12)

In reference to claim 17:

Caputo discloses a portable authorization device wherein:

- Each item of blended authorization information is derived from the two or more items of authorization information by performing an arithmetic operation on the two or more

items of authorization information, where the arithmetic operation is a modulus, and the items of authorization information are the PIN and the challenge received, and the blended authorization information may be the key, the encrypted data, encrypted using the key, or the final verification itself, which is also derived from two or more items of authorization information. Caputo (Column 17, lines 40-56)

In reference to claim 18:

Caputo discloses a method for operating a portable authorization device for selectively authorizing a host system to use one or more items of protected information comprising the steps of:

- Coupling the portable authorization device to the host system; Caputo(Figure 2, Item 12)
- Receiving a plurality of items of authorization information, where the items of authorization are the PIN, the key, and the challenge. Caputo(Column 17, Lines 37-56)
- Generating one or more items of blended authorization information from the plurality of items of authorization information, where the blended information is the encrypted key and PIN sent back in response to the challenge. Caputo(Column 17, Lines 37-56)
- Storing the one or more items of blended authorization information in a storage medium, where the authorization information is stored in the memory of the portable authorization device. Caputo(Column 17, Lines 37-56)
- Retrieving one or more of the items of blended authorization information from the storage medium. Caputo(Column 17, Lines 37-56)

- Regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information, where the challenger receives the information and regenerates the data by decrypting it. Caputo(Column 17, Lines 37-56)
- Selectively authorizing the host system to use an item of protected information based upon the at least one item of authorization information. Caputo(Column 17, Lines 37-56)

In reference to claim 19:

Caputo discloses a portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

- A processing unit; Caputo(Figure 2, Item 164)
- A first storage medium operatively coupled to the processing unit for storing one or more encoded items of authorization information; Caputo(Figure 2, Item 166)
- A second storage medium operatively coupled to the processing unit for storing decoding information used to decode the one or more encoded items of authorization information, wherein the second storage medium is accessible by the processing unit only if the processing unit receives proper authorization; Caputo(Column 14, Lines 57-65)
- A decoding mechanism operative in conjunction with the processing unit and the first and second storage media for decoding at least one of the one or more encoded items of authorization information to produce at least one respective item of authorization information, where the data is taken from the storage medium from the ROM/RAM, and

the smartcard, and enters a decryption module, or decoding mechanism. Caputo(Figure 4A)

- An interface operative in conjunction with the processing unit for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information. Caputo(Figure 2, Item 174)

Claims 20-27 have been canceled.

In reference to claim 28:

Caputo discloses a portable security device removably coupled to a computer system for selectively authorizing the computer system to use multiple items of protected information, comprising:

- A processing unit. (Figure 2, item 164)
- At least one storage medium couple to the processing unit. (Figure 2, Item 166)
- An interface capable of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information(Figure 2, items 178, 160, 176, 174), wherein the multiple items of authorization information are stored within the at least one memory (Figure 2, Items 166)
- An interface program for selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in memory, where the interface program is the authorization

software(Column 5, lines 7-13), the protected information is the application program, and the permission is based on authentication by PIN and challenge. (Column 17, lines 32-56)

In reference to claim 29:

Caputo discloses a method wherein the multiple items of authorization information comprise key selectors, where the multiple items of authorization information includes challenge and the PIN (Column 17, lines 32-56), and the PIN is the key selector (Column 14, lines 52-65)

In reference to claim 31:

Caputo discloses a method wherein the multiple items of authorization information comprise one or more secret keys(Column 13, lines 44-45), and the secret key is used in the authorization process as a digital signature verification. (Column 11, lines 49-59)

Claim 32 is a method substantially similar to the device of claim 28 and is rejected for the same reasons.

Claim 33 is rejected for the same reasons as claim 29.

Claim 35 is rejected for the same reasons as claim 31.

In reference to claim 36:

Caputo discloses a method for selectively authorizing the use of multiple items of protected information on a computer system, the method comprising the steps of:

- Providing a portable security device with at least one memory containing a shared secret and space for multiple key selectors, one key selector for each item of protected information, and at least one I/O port, whereby the key selectors can be downloaded into the security device, and communications can be established with the computer system, where the memory can hold a plurality of shared secrets and key selectors, and the key selectors may be downloaded into the device through user entry (Column 14, lines 52-65) & (Figure 2)
- Receiving by the portable security device an authorization request from the computer system to authorize use of a particular one of the items of protected information, where the authorization request is the challenge. (Column 17, lines 32-56)
- Using the stored key selector corresponding to the particular one of the items and the shared secret to generate authorizing information, wherein the computer system validates the authorizing information and releases the particular one of the items of protected information for use, where the shared secret is used for generating authorizing data through digital signature(Column 11, lines 49-59), and where the computer validates the information (Column 17, lines 32-56), and allows usage of protected information (Column 5, lines 7-12)

In reference to claim 37:

Caputo discloses a method further including the step of providing the key selectors to the portable security device memory using external information authorities within a secure transaction, where the external information authority is the user and the key selector entered into the portable security device is the PIN. (Column 17, lines 32-56)

In reference to claim 38:

Caputo discloses a method further including the step of receiving a random challenge from the information authority, using the shared secret to encrypt the response, and validating by the information authority the response by decrypting with the shared secret, where the challenger issues the challenge, and the response is encrypted (Column 17, lines 32-56), and decrypted for verification (Column 16, lines 51-54)

In reference to claim 39:

Caputo discloses a method where the shared secret is an encryption key. (Column 13, lines 44-48)

In reference to claim 40:

Caputo discloses the method further including the step of transforming the received key selector into an authorizing key using the shared secret key, where the received key selector is the PIN, the authorizing key is authentication process ACK, and the shared secret key is used to encrypt the PIN (Column 17, lines 39-56)

In reference to claim 41:

Caputo discloses a method where the authorization request is a randomly generated challenge number. (Column 17, lines 32-39)

In reference to claim 42:

Caputo discloses a method where the authorization information is generated by using the challenge and the authorizing key, where the authorizing key is the key used to encrypt the communications. (Column 17, lines 32-56)

In reference to claim 43:

Caputo discloses a method further including the step of encrypting the key selectors before storing in the portable security device memory, where the PIN as the key selector is preloaded into the memory. (Column 17, lines 24-27)

In reference to claim 44:

Caputo discloses a method further including the step of storing the key selectors in a merged pool in memory using a blending algorithm, whereby an individual key selector cannot be extracted from a specific location in memory, where the key selector is PIN is stored in an encrypted format (Column 13, lines 40-45) using DES (Column 11, line 5). Because DES, uses a series of S-BOXes and rotating bits, the key selector or PIN is blended and cannot be extracted from any specific location in memory. Examiner further notes, that any common encryption method involving the use of block ciphers would meet the "blending" of claim 44.

In reference to claim 45:

Caputo discloses a method further including the step of receiving the multiple items of information from multiple information authorities, where the multiple items of information are they challenge and the PIN. (Column 17, lines 32-56)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 30, 34 are rejected in view of Caputo.

In reference to claim 30:

Caputo discloses a method wherein selective authorization is given to the computer system to use multiple items of protected information based upon the key. (Column 17, lines 32-56)

Caputo fails to explicitly disclose a method wherein a key is generated within the portable security device based upon the key selectors.

The examiner takes official notice that generating a key in either side of an authentication scheme was well known at the time of invention. Authentication involves either then authentication, and subsequent authorization of either the client, the server, or the client and server. Public key authentication schemes in particular often use a key generation technique in which the key is generated on both sides using a seed or initial value to avoid the key from being compromised through insecure transmission.

It would have been obvious to one of ordinary skill in the art at the time of invention to generate the key inside of the portable device in order to avoid transmitting the key over an insecure line and leave the possibility open for the private key becoming compromised.

Claim 34 is rejected for the same reasons as claim 30.

Conclusion

6. The following art not relied upon is made of record.

- US patent 5568552 discloses a method of moving a software license from one node to another.
- US patent 6671808 discloses a USB compliant dongle.
- US patent 5222133 discloses a method of using multiple items of authorization information to authorize a single software package.
- US patent 5754761 discloses a universal software key which can authorize different pieces of software.

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

Customer Service Representative Telephone: 571-272-2100 Fax: 703-872-9306

TMH

February 6th, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100